Listing of Claims:

1. (original) A computer system adapted to restrict operations on data, comprising:

a computer platform having a secure operator for checking whether a user of the platform is licensed to perform a requested operation on the data and for enabling use of the data;

a portable trusted module containing a user identity, wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorized external modification;

and an access profile specifying license permissions of users with respect to the data;

wherein the secure operator is adapted to check the access profile to determine whether a requested operation is licensed for the user identity contained in the portable trusted module and prevent the requested operation if a license is required and not present.

2. (original) A computer system as claimed in claim 1, wherein the computer platform further comprises a platform trusted module, and wherein the platform trusted module and the portable trusted module are adapted for mutual authentication.

3. (original) A computer system as claimed in claim 2, wherein some or all of the functionality of the secure operator is within the platform trusted module.

4. (previously presented) A computer system as claimed in claim 1, wherein the access profile is within the computer platform.

5. (previously presented) A computer system as claimed in claim 1, wherein some or all of the data is within the computer platform, and the computer platform further comprises a data protector for checking data integrity before a processor of the computer platform carries out operations on the data.

6. (previously presented) A computer system as claimed in claim 1, wherein some or all of the data is within the portable trusted module or in a device containing the portable trusted module, and the portable trusted module or the device containing the portable trusted module further comprises a data protector for checking data integrity before a processor of the computer platform carries out operations on the data.

7. (previously presented) A computer system as claimed in claim 5, wherein the data protector is within the relevant trusted module.

8. (previously presented) A computer system as claimed in claim 5, wherein the data protector is adapted to check installation of data and to load a digest of protected data and/or any associated access profile into the relevant trusted component.

9. (previously presented) A computer system as claimed in claim 1, wherein the trusted platform is adapted at boot to check the integrity of operation protection code comprising the secure operator and, if present, the data protector.

10. (previously presented) A computer system as claimed in claim 9, wherein the computer platform further comprises a platform trusted module, and wherein the platform trusted module and the portable trusted module are adapted for mutual authentication, and wherein the computer platform is adapted to perform the integrity check by reading and hashing the operation protection code to produce a first hash, reading and decrypting a stored signed version of a secure operation protection code hash using a public key certificate of a third party stored in the platform trusted module to produce a second hash, and comparing the first hash and the second hash.

11. (previously presented) A computer system as claimed in claim 1, wherein the portable trusted module contains a user access license specifying access rights to the data associated with the removable trusted module, whereby unless prevented by the access profile, the secure operator is adapted to check the user access license to determine whether a requested operation is licensed for the user identity contained in the portable trusted module.

12. (previously presented) A computer system as claimed in claim 2, wherein the computer platform comprises a secure communication path between the platform trusted module and the operating system of the computer platform.

13. (currently amended) A computer system as claimed in claim 1, wherein the computer platform is adapted such that:

the operating system requests a policy check from the secure operator before acting upon the data, by sending the name of the target data plus the intended operation;

the secure operator checks the restrictions associated with the target data in the access profile, to determine whether the data may be operated upon; and

the secure operator checks the proposed usage with the restrictions, and replies to the operating system.

14. (currently amended) A computer system as claimed in claim 13, wherein the computer platform further comprises a platform trusted module, wherein the platform trusted module and the portable trusted module are adapted for mutual authentication[[.]], and wherein some or all of the functionality of the secure operator is within the platform trusted module; wherein on request by the operating system for permission to operate on the data, the secure operator sends a message to the access profile signed with a private key of the platform trusted module, wherein the access profile has access to the public key of the platform trusted module and can verify and authenticate the signed message with said public key, whereby if satisfied the access profile sends access profile sends access profile data to the secure operator, whereupon the secure operator tests the access profile data and if appropriate requests the operating system to carry out the operation requested.

15. (previously presented) A computer system as claimed in claim 13, wherein the computer platform further comprises a platform trusted module, and wherein the platform trusted module

and the portable trusted module are adapted for mutual authentication, and wherein the computer system further comprises a data protector for checking data integrity before a processor of the computer platform carries out operations on the data; wherein the relevant trusted component contains a secure result of a one-way function on the data and associated access profile, and the data protector prevents the operation from being carried out if calculation of the one-way function provides a result different from the secure result.

16. (previously presented) A computer system as claimed in claim 2, wherein the platform trusted component is adapted to log requests to the operating system to perform particular operations on the data.

17. (original) A computer system as claimed in claim 6, wherein the portable trusted component is adapted to log requests to the operating system to perform particular operations on the data.

18. (previously presented) A computer system adapted to restrict operations on data, comprising:

a computer platform having an access controller for specifying license permissions of users with respect to the data and for enabling use of the data;

a portable trusted module containing a user identity, wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorized external modification;

wherein the access controller is adapted to determine whether a requested operation is licensed for the user identity contained in the portable trusted module and prevent the requested operation if a license is required and not present.

19. (previously presented) A computer system as claimed in claim 18, wherein the operating system of the computer platform is adapted to request a policy check from the access controller before carrying out certain operations on the data, whereupon the access controller checks

restrictions applying to the data to determine whether the data may be operated on, and replies to the operating system accordingly.

20. (currently amended) A method of restricting operations on data in a system comprising:

computer platform having a secure operator for checking whether a user of the platform is licensed to perform a requested operation on the data and for enabling use of the data;

a portable trusted module containing a user identity, wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorised external modification;

and an access profile specifying license permissions of users with respect to the data;

the method comprising a request for a policy check by the operating system of the computer platform to the secure operator before acting upon the data, by sending to the secure operator the name of the target data plus the intended operation;

the secure operator checking the restrictions associated with the target data in the access profile to determine whether the data may be operated upon; and

the secure operator checking the proposed usage with the restrictions, and replying to the operating system.

21. (original): A method as claimed in claim 20, wherein the computer platform further comprises a platform trusted module, and wherein some or all of the functionality of the secure operator is within the platform trusted module, and whereby on request by the operating system for permission to operate on the data, the secure operator sends a message to the access profile signed with a private key of the platform trusted module, wherein the access profile has access to the public key of the platform trusted module and can verify and authenticate the signed message with said public key, whereby if satisfied the access profile sends access profile data to the secure

operator, whereupon the secure operator tests the access profile data and if appropriate requests the operating system to carry out the operation requested.

22. (currently amended) A method as claimed in claim 21, wherein the [[the]] computer platform further comprises a data protector for checking data integrity before a processor of the computer platform carries out operation on the data, and wherein [[wherein]] the platform trusted component contains a secure result of a one-way function on the data and associated access profile, and the data protector prevents the operation from being carried out if calculation of the one-way function provides a result different from the secure result.

23. (original) A method as claimed in claim 21, wherein before execution of the data, the data protector checks that there are not multiple copies of the data stored within the computer platform and prevents data execution if there are multiple copies.

24. (original) A method as claimed in claim 21, wherein the computer platform comprises a secure communication path between the platform trusted component and the operating system, and whereby the request from the secure operator to the operating system to use the data is provided on the secure communication path.

25. (original) A method as claimed in claim 21, wherein the platform trusted module is adapted to log any request to the operating system to perform a particular operation on the data.

26. (original) A method of installing data on to a computer platform for restricted use thereon, the computer platform comprising: a computer platform having a secure operator for checking whether a user of the platform is licensed to perform a requested operation on the data and for enabling use of the data, a platform trusted module wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorised external modification, and a data protector for checking data integrity before a processor of the computer platform carries out operations on the data; the method comprising verification of the reliability of the data before installation of the data and an associated access profile and loading of a digest of protected data

and an associated access profile into the platform trusted module, whereby the digest is used by the data protector and/or secure operator before execution of the data.

27. (original) A computer platform having a secure operator for checking whether a user of the platform is licensed to perform a requested operation on the data and for enabling use of the data and access profile specifying license permissions of users with respect to the data; wherein the secure operator is adapted to check the access profile to determine whether a requested operation is licensed for a user identity contained in a portable trusted module in communication with the computer platform, wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorised external modification, and prevent the requested operation if a license is required and not present.

28. (original) A computer platform as claimed in claim 27, further comprising a platform trusted module, and wherein the platform trusted module and the portable trusted module are adapted for mutual authentication.

29. (original) A computer platform as claimed in claim 28, wherein some or all of the functionality of the secure operator is within the platform trusted module.

30. (previously presented) A computer platform as claimed in claim 27, wherein the access profile is within the platform trusted module.

31. (previously presented) A computer platform as claimed in claim 27, wherein some or all of the data is within the computer platform, and the computer platform further comprises a data protector for checking data integrity before a processor of the computer platform carries out operations on the data.

32. (original) A computer platform as claimed in claim 31, wherein the data protector is within the platform trusted module.

33. (previously presented) A computer platform as claimed in claim 31, wherein the data protector is adapted to check installation of data and to load a digest of protected data and/or any associated access profile into the platform trusted component.

34. (previously presented) A computer platform as claimed in claim 27, wherein the computer platform is adapted at boot to check the integrity of operation protection code comprising the secure operator and, if present, the data protector.

35. (original) A computer platform as claimed in claim 28, further comprising a secure communication path between the platform trusted module and the operating system of the computer platform.

36. (currently amended) A computer platform as claimed in claim 27, adapted such that:

the operating system requests a policy check from the secure operator before acting upon the data, by sending the name of the data plus the intended operation;

the secure operator checks the restrictions associated with the target data in the access profile, to determine whether the data may be operated upon; and

the secure operator checks the proposed usage with the restrictions, and replies to the operating system.

37. (previously presented) A computer platform as claimed in claim 36, further comprising a platform trusted module, and wherein the platform trusted module and the portable trusted module are adapted for mutual authentication, wherein on request by the operating system for permission to operate on the data, the secure operator sends a message to the access profile signed with a private key of the platform trusted module, wherein the access profile has access to the public key of the platform trusted module and can verify and authenticate the signed message with said public key, whereby if satisfied the access profile sends access profile data to the secure operator,

whereupon the secure operator tests the access profile data and if appropriate requests the operating system to carry out the operation requested.

38. (previously presented) A computer platform as claimed in claim 31, further comprising a platform trusted module, and wherein the platform trusted module and the portable trusted module are adapted for mutual authentication, wherein the platform trusted component contains a secure result of a one-way function on the data and associated access profile, and the data protector prevents the operation from being carried out if calculation of the one-way function provides a result different from the secure result.

39. (currently amended) A portable trusted module containing a user identity, wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorised external modification; the portable trusted module containing a user access license specifying access rights to data associated with the ~~removable~~ portable trusted module.

40. (original) A portable trusted module as claimed in claim 39 and located within a smart card.

41. (currently amended) A method of restricting operations on data in a system comprising:

a computer platform having an access controller specifying license permissions of users with respect to the data; and for enabling use of the data;

a portable trusted module containing a user identity, wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorised external modification;

the method comprising a request for a policy check by the operating system of the computer platform to the access controller before acting upon the data, by sending to the access controller the name of the target data plus the intended operation;

the access controller checking the restrictions associated with the target data to determine whether the data may be operated upon; and

replying to the operating system.

42. (previously presented) A method as claimed in claim 41, wherein the computer platform further comprises a platform trusted module, and wherein some or all of the functionality of the access controller is within the platform trusted module.

43. (previously presented) A computer system as claimed in claim 6, wherein the data protector is within the relevant trusted module.

44. (previously presented) A computer system as claimed in claim 6, wherein the data protector is adapted to check installation of data and to load a digest of protected data and/or any associated access profile into the relevant trusted component.